Arnold Mathematical Journal
Volume 11, Issue 1, 2025

A Simple Construction of the Field of Witt Vectors

Vladimir Fock

Received 10 Mar 2024; Accepted 10 Oct 2024

Abstract: We present a short, hopefully pedagogical construction of the field and ring of Witt vectors. It uses a natural binary operation on polynomials of one variable, which we call *convolution*.

AMS Classification: 13F35

Key words and phrases: Arithmetic rings, Witt vectors

Introduction

Witt vectors form a field of characteristic 0 constructed out of a field of finite characteristic p. This construction suggested by E. Witt [Wit37] in 1936 generalizes the field $\mathbb{Q}_p$ of p-adic rationals. His construction has a reputation to be complicated and counter-intuitive. We suggest a very concise version of construction of Witt vectors. It is inspired by a paper by D.Kaledin [Kal12] who observed a relation between Witt vectors and the tame symbol in disguise of the so-called Japanese cocycle.

DOI: 10.56994/ARMJ.011.001.001

In the wikipedia article on Witt vectors (july 2024) it is indicated that "they have a highly non-intuitive structure". The aim of this note is to refute this claim.

A very similar construction is essentially contained in the notes by Michiel Hazewinkel [Haz09], mainly in the section 9 and the section 14. This review contains a lot of information for further reading on the subject.

Convolution

We are going to define a binary operation on polynomials of one variable modifying the definition of a resultant.

Let $f(t) = 1 + a_1 t + \cdots$ and $g(t) = 1 + b_1 t + \cdots$ belong to the multiplicative semi-group $1 + t\mathbb{F}[t]$ of polynomials with coefficients in a field $\mathbb{F}$ and the constant term equal to 1. Define a *convolution* $f \star g$ as a polynomial with the constant term 1 and having as roots the products of one root of f and one of g. In other words, suppose that $f(t) = \prod_i (1 - \lambda_i t)$ and $g(t) = \prod_j (1 - \mu_j t)$ with λ_i, μ_j belonging to the algebraic closure of the field $\mathbb{F}$. Then

$$f \star g\,(t) = \prod_{ij}(1 - t\lambda_i\mu_j) = \prod_i g(\lambda_i t) = \prod_j f(\mu_j t).$$

The convolution can also be expressed in term of the resultant, namely

$$f \star g\,(t) = \mathtt{res}_z(f(z), z^{\deg g} g(t/z)).$$

To give an equivalent definition, consider the ring $\mathbb{F}[x,y]/(f(x)) + (g(y))$ and denote by $\hat{x}^{-1}$ and $\hat{y}^{-1}$ the multiplication in this ring by x^{-1} and y^{-1}, respectively. In the standard basis they are given by matrices with entries in $\mathbb{F}$. Then

$$f \star g\,(t) = \det(1 - t\hat{x}^{-1}\hat{y}^{-1}).$$

In this definition it is explicit that the coefficients of $f \star g$ are polynomial functions of those of f and g.

The fourth definition works for $\mathbb{F} = \mathbb{C}$ and shows the relation to the tame symbol. Consider a curve γ around zero on the complex plane sufficiently small in order not to surround any root of $f(z)$. The convolution can be defined by the formula (see P.Deligne [Del91], formula 2.7.2)

$$f \star g\,(t) = \{f(z), g(t/z)\}_\gamma = \exp\left(\frac{1}{2\pi i}\int_\gamma \ln f(z) d\ln g(t/z)\right)$$

valid for t so small that all roots of $g(t/z)$ are inside the curve γ.

The convolution enjoys the following properties obvious from the definitions:

1. $\deg(f \star g) = \deg f \deg g$,
2. $f \star 1 = 1$,
3. $f \star (1 - t) = f$,
4. $(1 - at) \star (1 - bt) = (1 - abt)$,
5. $f \star g = g \star f$,
6. $f \star (g_1 g_2) = (f \star g_1)(f \star g_2)$.

These properties imply that the semi-group $1 + t\mathbb{F}[t]$ is a commutative semi-ring with respect to the multiplication as a semi-ring addition and convolution as a semi-ring multiplication. The multiplicativity property 6 is just the expression of the distributive law of the semi-ring.

The following property is also an easy consequence of the definition:

- The set $1 + t^n\mathbb{F}[t]$ is an ideal.

This property implies that the convolution can be extended to the group of formal power series $1 + t\mathbb{F}[[t]]$ providing it with a ring structure. This ring is called the ring of the *universal* or *big* Witt vectors and is denoted by $W(\mathbb{F})$, see [Haz09], section 9.

Witt vectors

The aim of this paragraph is to give a concise definition of the Witt ring.

For that we need just another property of the universal Witt ring obviously following from the definition of the convolution:

- The set $1 + t^n\mathbb{F}[[t^n]]$ is also an ideal.

Let $\mathbb{F}$ be a field of characteristic p and let $W(\mathbb{F})$ be the corresponding universal Witt ring.

Define the *Witt ring* $W_{\mathbb{F}}$ as a quotient

$$W_{\mathbb{F}} = W(\mathbb{F}) / \prod_{n>1|n\neq p^k}(1 + t^n\mathbb{F}[[t^n]]).$$

Here we used the property and denoted the sum of ideals multiplicatively since it corresponds to the product of the series.

Observe that any element of the group $1 + t\mathbb{F}[[t]]$ can be presented either as a sum $1 + \alpha_1 t + \alpha_2 t^2 + \cdots$ or as a product $(1 - a_1 t)(1 - a_2 t^2)(1 - a_3 t^3)\cdots$.

Using the latter presentation the elements of the ring $W_{\mathbb{F}}$ can be uniquely represented as formal products

$$f(t) = \prod_{i=0}^{\infty}(1 - a_i t^{p^i}).$$

In this presentation certain properties of the Witt vectors become obvious. In particular, it follows from the property 4 that the correspondence $a \longmapsto (1 - at)$ gives an embedding of multiplicative groups $\mathbb{F}^\times \to W_{\mathbb{F}}^\times$. The images of the elements of $\mathbb{F}^\times$ are called their *Teichmüller representatives.* It is also obvious that the ring multiplication by p in the ring $W_{\mathbb{F}}$ amounts to the shift of the coefficients a_i composed with the Frobenius automorphism:

$$\prod_{i=0}^{\infty}(1 - a_i t^{p^i}) \longmapsto \prod_{i=1}^{\infty}(1 - a_{i-1}^p t^{p^i}).$$

This property allows to identify the field of fractions of the ring $W_{\mathbb{F}}$ with the expressions of the form

$$\prod_{i=N}^{\infty}(1 - a_i t^{p^i})$$

with possibly negative N.

Recall that for a field $\mathbb{F}_p$ of p elements the ring $W_{\mathbb{F}}$ coincides with the ring $\mathbb{Z}_p$ of p-adic integers.

Relation to the standard definition of the Witt vectors

Consider the ring of formal series $\mathbb{C}[[t]]^{+\circ}$ with respect to addition and coefficentwise (Hadamard) multiplication denoted by $\circ$ defined as

$$(\sum_{k=0}^{\infty} a_k t^k)\circ(\sum_{k=0}^{\infty} b_k t^k) = \sum_{k=0}^{\infty} a_k b_k t^k$$

Clearly this ring is just a direct sum of infinitely many copies of the ring $\mathbb{C}$.

The map $f \longmapsto -f'/f$ gives an isomorphism between the rings $(1+\mathbb{C}[[t]])^{\cdot\star}$ and $\mathbb{C}[[t]]^{+\circ}$. Indeed

$$\begin{aligned}(-f'/f)\circ(-g'/g) &= \left(\sum_{k=1}^{\infty}(\sum_i \lambda_i^k)t^{k-1}\right)\circ\left(\sum_{k=0}^{\infty}(\sum_j \mu_j^k)t^{k-1}\right) = \\ &= \left(\sum_k(\sum_{ij}\lambda_i^k\mu_j^k)t^{k-1}\right) = -(f\star g)'/(f\star g),\end{aligned}$$

and obviously

$$-f'/f - g'/g = -(fg)'/(fg).$$

In the explicit coordinates we have

$$\prod(1-a_i t^i) \longmapsto \sum_i\sum_k a_i^k t^{ik-1} = \sum_l \sum_{i|l} i a_i^{l/i} t^{l-1}.$$

The expressions

$$S_l(a_1, a_2, \ldots) = \sum_{i|l} i a_i^{i/l}$$

are called the *universal Witt polynomials* (P. Cartier [Car67] and [Haz09] section 9). We see that each of the Witt polynomials gives a homomorphism from the universal Witt ring to the ring of complex numbers and a collection of all such polynomials gives an isomorphism of the universal Witt ring to the infinite sum of complex numbers. The standard construction uses this isomorphism to define the ring structure in terms of the coefficients a_i. Then one proves that the product and the sum are in fact given by algebraic expressions with integer coefficients and thus are defined over any field.

References

[Car67] Pierre Cartier. Groupes formels associés aux anneaux de Witt généralisés. *C. R. Acad. Sci. Paris Sér. A-B*, 265:A49–A52, 1967. 5

[Del91] P. Deligne. Le symbole modéré. *Inst. Hautes Études Sci. Publ. Math.*, (73):147–181, 1991. 3

[Haz09] Michiel Hazewinkel. Witt vectors. I. In *Handbook of algebra*, volume 6, pages 319–472. 2009. 2, 3, 5

[Kal12] D. Kaledin. Universal Witt vectors and the "Japanese cocycle". *Mosc. Math. J.*, 12(3):593–604, 669, 2012. 1

[Wit37] Ernst Witt. Zyklische Körper und Algebren der Charakteristik p vom Grad pn. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p. *Journal für die Reine und Angewandte Mathematik*, 1937(176):126–140, 1937. 1

AUTHOR

Vladimir Fock,
IRMA, Université de Strasbourg, France,
email: fock@math.unistra.fr